R E M A R K S

Reconsideration of this application, as amended, is respectfully requested.

THE SPECIFICATION

The specification has been amended to correct some minor informalities of which the undersigned has become aware.

No new matter has been added, and it is respectfully requested that the amendments to the specification be approved and entered.

THE DRAWINGS

It is respectfully submitted that the drawings filed with the application papers on March 15, 2004, are formal and it is respectfully requested that the Examiner indicate the drawings as being accepted in the next Office Action.

THE CLAIMS

Claims 1-6 have been canceled without prejudice and claim 14 has been amended to overcome the rejection under 35 USC 112.

In addition, the claims have been amended to make some minor grammatical improvements and to correct some minor antecedent basis problems so as to put them in better form for issuance in a U.S. patent.

No new matter has been added, and it is respectfully requested that the amendments to the claims be approved and entered and that the 35 USC 112 rejection be withdrawn.

It is respectfully submitted, moreover, that the amendments to the claims are not related to patentability, and do not narrow the scope of the claims either literally or under the doctrine of equivalents.

THE PRIOR ART REJECTION

Claims 1-19 were rejected under 35 USC 102 as being anticipated by USP 7,155,012 ("Candelore et al"), and claim 20 was rejected under 35 USC 103 as being obvious over Candelore et al. These rejections, however, are respectfully traversed.

Significantly, according to the present invention as recited in independent claim 7, a data decoding device is provided which extracts a portion of compressed data encryption key data, encrypts the extracted portion, and then decodes the encrypted data back to the compressed data by combining the encryption key data and the encrypted data, both of which have been generated from the same compressed data.

According to the present invention as recited in each of independent claims 8 and 20, moreover, the encryption key data is stored in an encryption key storage means; management information showing a correspondence between the encryption key data and the

encrypted data, which have been acquired for the same compressed data, is stored in the management information storing means; and the encryption key data and the encrypted data, both of which have been acquired from the same compressed data, are extracted from the respective storage means based on the management information stored in the management information storing means, and the extracted encryption key data and the extracted encrypted data are combined and decoded back to the compressed data.

Still further, according to the present invention as recited in independent claim 13, the encryption key data and specific information which identifies the encrypted data corresponding to the encryption key data is output in a predetermined form to an external user.

Thus, according to the present invention as recited in each of amended independent claims 7, 8, 13 and 20, high-volume image data (for example, page data) is compressed, a portion of the compressed image data is extracted as encryption key data, and the portion of the compressed image data, which corresponds to the extracted encryption key data, is changed (for example, replaced with other data, deleted, etc.) so as to prevent expansion (i.e., decompression/decoding) of the compressed image data back to original image data. With this structure of the claimed present invention, it becomes impossible to expand/decompress/decode the compressed image data which has been

encrypted by partially changing the portion of the compressed image data, without the corresponding encryption key data. As a result, unauthorized reproduction of the original image data from the compressed image data can be prevented.

With respect to the cited prior art, Candelore et al merely discloses a mechanism for scrambling contents of a cable television or satellite broadcasting signal by, for example, encrypting data corresponding to stripes or a mosaic in an image of the broadcasting signal, in order to inhibit unauthorized use of content by subscribers. More specifically, in Candelore et al, specific packet data from a video signal such a luminance, chroma or audio signal is selected, and then the selected packet data is encrypted.

However, it is respectfully submitted that Candelore et al does not disclose, teach or suggest the feature of the present invention as recited in independent claim 7 whereby encrypted data is decoded back to the compressed data by <u>combining the encryption key data and the encrypted data, both of which have been generated from the same compressed data</u>.

In addition, it is respectfully submitted that Candelore et al does not disclose, teach or suggest the features of the present invention as recited in independent claims 8 and 20 whereby: encryption key data is stored in an encryption key storage means; management information showing correspondence

between the encryption key data and the encrypted data which have been acquired for the same compressed data is stored in the management information storing means; and the encryption key data and the encrypted data, both of which have been acquired from the same compressed data, are extracted from the respective storage means based on the management information stored in the management information storing means, and the extracted encryption key data and the extracted encrypted data are combined and decoded back to the compressed data.

And still further, it is respectfully submitted that Candelore et al does not disclose, teach or suggest the feature of the present invention as recited in independent claim 13 whereby encryption key data and specific information which identifies the encrypted data corresponding to the encryption key data is output in a predetermined form to an external user.

In view of the foregoing, it is respectfully submitted that the present invention as recited in each of independent claims 7, 8, 13 and 20, and claims 9-12 and 14-19 respectively depending therefrom, clearly patentably distinguishes over Canedlore et al under 35 USC 102 as well as under 35 USC 103.

* *

Entry of this Amendment, allowance of the claims and the passing of this application to issue are respectfully solicited.

   If the Examiner has any comments, questions, objections or recommendations, the Examiner is invited to telephone the undersigned at the telephone number given below for prompt action.

                              Respectfully submitted,

                              /Douglas Holtz/

                              Douglas Holtz
                              Reg. No. 33,902

Frishauf, Holtz, Goodman & Chick, P.C.
220 Fifth Avenue – 16th Floor
New York, New York 10001-7708
Tel. No. (212) 319-4900
Fax No. (212) 319-5101

DH:jd
encs.